Abstract of the Invention

A method for communicating confidential data over a computer network, such as the Internet includes encrypting the confidential data while the confidential data is in the control of a sender. The step of encrypting includes mixing the confidential data with biometric data to produce encrypted data. The encrypted data is then sent over a communication link to a receiver. The encrypted data is de-encrypted while the encrypted data is in the control of the receiver by separating the biometric data from the confidential data. Voice signatures are convenient forms of biometric data and may be used for the dual purpose of encrypting the data to be sent and serving as a key to be matched by the second entity to gain access to the data, i.e., to allow de-encryption. The further step of converting the encrypted data from a first format to a second format, e.g., wave file format, may provide additional security and requires the reconversion by the second entity in order to de-encrypt. Additional key data may be generated and combined with the confidential data and/or biometric data in accordance with a predetermined algorithm to create a second level of encryption and which is de-encrypted by a reverse algorithm.